REMARKS

The Examiner has objected to the specification for containing an embedded hyperlink on Page 2, line 1. Applicant respectfully asserts that such objection has been avoided by virtue of the amendment made hereinabove to the specification.

The Examiner has rejected Claims 1-3, 5-10, 13-14, 16-18, 20-25, 28-29, 31 and 55 under 35 U.S.C. 103(a) as being unpatentable over Trkca et al. (U.S. Patent No. 6,453,345) in view of Stevens (TCP/IP Illustrated). In addition, the Examiner has rejected Claims 4, 19, 32-38, 40-47 and 49-52 under 35 U.S.C. 103(a) as being unpatentable over Trkca, in view of Stevens, in further view of Cheriton (U.S. Patent No. 7,054,930). Applicant respectfully disagrees with such rejection.

With respect to independent Claims 1 and 16, the Examiner has relied on Pages 6-11 in Stevens to make a prior art showing of applicant's claimed "reassembling one or more of the incoming datagrams into a segment structured in compliance with a transport protocol layer" (see the same or similar, but not necessarily identical language in the aforementioned independent claims).

Specifically, the Examiner has argued that "[i]t was well known that in the Internet Protocol there are multiple layers and that each layer contains different modules, such as the TCP module and the UDP module of the transport layer" and that "[i]t was also well known that in order to get to the data in the application layer packet, such as the payload and the packet type, the transport layer module must process the transport layer packet to reveal the application layer packet," as "evidenced by Stevens Pages 6-11."

Applicant respectfully disagrees. First, applicant respectfully asserts that the excerpt from Stevens relied on by the Examiner merely relates to TCP/IP layering (see Page 6) and states that "[t]here are more protocols in the TCP/IP protocol suite" (see Page 6) "at different layers in the TCP/IP protocol suite" (see Figure 1.4 caption on Page 6). Clearly, only disclosing that multiple protocols exist at different layers in the TCP/IP

protocol suite, as in Stevens, fails to specifically teach "**reassembling** one or more of the incoming datagrams into a segment structured in compliance with a transport protocol layer" (emphasis added), as claimed.

Second, it also seems that the Examiner has relied on an Official Notice argument to reject applicant's specific claim language. For example, applicant notes that the Examiner has stated that "[i]t was also well known that in order to get to the data in the application layer packet, such as the payload and the packet type, the transport layer module must process the transport layer packet to reveal the application layer packet," as noted above. Applicant respectfully asserts that simply arguing that it was well known to process a transport layer packet to reveal an application layer packet, as noted by the Examiner, fails to even suggest "**reassembling** one or more of the **incoming datagrams** into a segment structured in compliance with a transport protocol layer" (emphasis added), as claimed.

Thus, in response to the Examiner's apparent reliance on Official Notice in rejecting applicant's specific claim language, applicant again points out the remarks above that clearly show the manner in which some of such claims further distinguish Trcka. Applicant thus formally requests a specific showing of the subject matter in ALL of the claims in any future action. Note excerpt from MPEP below.

"If the applicant traverses such an [Official Notice] assertion the examiner should cite a reference in support of his or her position." See MPEP 2144.03.

With respect to independent Claim 1, the Examiner has relied on the following excerpt from Trcka to make a prior art showing of applicant's claimed "protocol-specific module processing each reassembled datagram based on the transport protocol layer employed by the reassembled datagram."

"With further reference to FIG. 3, the Post-Capture Processing Module 98 serves in-part as an interface to the traffic analysis databases 96. These databases are used by the analysis applications 100 to store and manipulate selected portions of

> traffic data. In operation, archived traffic data is loaded into the traffic analysis databases 96 from the Data Playback Unit 68. Traffic data can also be loaded into the databases 96 from either of the cyclic recorders 82, 84. As the raw traffic data is read-in by the controller 64, the Post-Capture Processing Module 98 decrypts the data (if the data is encrypted), and filters-out packets based on user-specified criteria; in addition, to facilitate the subsequent analysis of the data, the Post-Capture Processing Module 98 processes the packets based on protocol-specific packet fields to build various transaction data structures and records that represent the various application and user transactions. The Post-Capture Processing Module 98 is described in further detail below." (Col. 13, lines 32-49-emphasis added)

Applicant respectfully asserts that the excerpt from Trcka relied on by the Examiner merely discloses that a "Post-Capture Processing Module 98 processes the packets based on protocol-specific packet fields." Clearly, only generally disclosing a module that processes packets based on protocol specific packet fields, as in Trcka, fails to meet applicant's claimed "protocol-**specific** module processing each reassembled datagram based on the transport protocol layer employed by the reassembled datagram" (emphasis added), as claimed.

With respect to independent Claims 32 and 41, the Examiner has relied on Col. 2, lines 29-34; Col. 4, lines 2-11; Col. 7, lines 28-32; and Col. 12, lines 29-40 in Trcka to make a prior art showing of applicant's claimed "receiving copies of datagrams transiting a boundary of a network domain into an incoming packet queue" (see the same or similar, but not necessarily identical language in the aforementioned independent claims).

Applicant respectfully asserts that the excerpts from Trcka relied on by the Examiner simply teach that "the system captures and records the packets passively" (Col. 2, lines 30-31), "software which continuously routes at least some of the passively-captured traffic data to a cyclic data recorder" (Col. 4, lines 4-5), "[t]he archival recording generated by the above-described process is in essence a complete replica of all valid network traffic" (Col. 7, lines 28-30), and "the archival data stream generated by the Archival Data Processing Module 90…is…routed to…enable the automated analysis of such data" (Col. 12, lines 29-33).

Only generally disclosing capturing and recording packets, as in Trcka, does not teach "receiving copies of datagrams transiting a boundary of a network domain" (emphasis added), as claimed. In fact, Trcka expressly discloses that the archival recording is in essence a complete replica of all valid network traffic, as noted above, which does not meet applicant's specifically claimed "receiving copies of datagrams transiting a boundary of a network domain" (emphasis added), as claimed.

Still with respect to independent Claims 32 and 41, the Examiner has relied on the following excerpt from Trcka to make a prior art showing of applicant's claimed technique of "each datagram being copied from a packet stream" (see the same or similar, but not necessarily identical language in the aforementioned independent claims).

> "As discussed below, the original timing of the incoming packet stream is nevertheless preserved by inserting the date/time stamps into the packet stream." (Col. 14, lines 34-36)

Applicant respectfully asserts that only disclosing that the original timing of the incoming packet stream is preserved by inserting the date/time stamps into the packet stream, as in Trcka, fails to even suggest any sort of copying, let alone that "each datagram [is] copied from a packet stream," as claimed.

Further, with respect to independent Claims 32 and 41, the Examiner has relied on Pages 4-11 in Stevens in addition to the rejection of Claim 1 to make a prior art showing of applicant's claimed "reassembling one or more such datagrams from the incoming packet queue into network protocol packets, each staged in a reassembled packet queue" (see the same or similar, but not necessarily identical language in the aforementioned independent claims).

First, applicant respectfully asserts that the excerpt from Stevens relied on by the Examiner merely relates to TCP/IP layering (see Page 6) and states that "[t]here are more protocols in the TCP/IP protocol suite" (see Page 6) "at different layers in the TCP/IP protocol suite" (see Figure 1.4 caption on Page 6). Clearly, only disclosing that multiple protocols exist at different layers in the TCP/IP protocol suite, as in Stevens, fails to

specifically teach "**reassembling** one or more such datagrams," and particularly not "reassembling one or more such datagrams from the incoming packet queue into network protocol packets, each staged in a reassembled packet queue" (emphasis added), as claimed. Applicant emphasizes that Pages 4-11 in Stevens, as relied on by the Examiner, does not even suggest any sort of reassembling, incoming packet queue or reassembled packet queue, and especially not in the manner claimed by applicant.

Second, it also seems that the Examiner has relied on an Official Notice argument to reject applicant's specific claim language. For example, applicant notes that the Examiner has stated in the rejection of Claim 1 relied on by the Examiner that "[i]t was also well known that in order to get to the data in the application layer packet, such as the payload and the packet type, the transport layer module must process the transport layer packet to reveal the application layer packet," as noted above. Applicant respectfully asserts that simply arguing that it was well known to process a transport layer packet to reveal an application layer packet, as noted by the Examiner, fails to even suggest "**reassembling** one or more such datagrams from the incoming packet queue into network protocol packets, each staged in a reassembled packet queue" (emphasis added), as claimed.

Thus, in response to the Examiner's apparent reliance on Official Notice in rejecting applicant's specific claim language, applicant again points out the remarks above that clearly show the manner in which some of such claims further distinguish Trcka. Applicant thus formally requests a specific showing of the subject matter in ALL of the claims in any future action. See MPEP 2144.03 above.

Moreover, with respect to independent Claims 32 and 41, the Examiner has relied on Col. 3, line 66-Col. 4, line 16 in Trcka to make a prior art showing of applicant's claimed "scanning each network protocol packet from the reassembled packet queue to ascertain an infection of at least one of a computer virus and malware" (see the same or similar, but not necessarily identical language in the aforementioned independent claims).

Applicant respectfully asserts that such excerpt from Trcka only discloses that "a real-time monitoring application reads the traffic data from the cyclic recorder on a first-in-first-out basis and checks for pre-programmed anomalies." However, applicant notes that Trcka only discloses "software which continuously routes at least some of the passively-captured traffic data to a cyclic data recorder" (Col. 4, lines 3-5).

Thus, the excerpt from Trcka relied on by the Examiner only discloses reading traffic data from a cyclic recorder on a first-in-first-out basis and checking such traffic data for pre-programmed anomalies, where the traffic data read from the cyclic recorder includes passively-captured traffic data. To this end, applicant respectfully points out that checking passively-captured traffic data stored in a cyclic recorder, as in Trcka, fails to specifically meet applicant's claimed "scanning each network protocol packet from the **reassembled** packet queue to ascertain an infection of at least one of a computer virus and malware" (emphasis added), particularly where "reassembl[ed]…datagrams [are] each staged in [the] reassembled packet queue," in the context claimed by applicant.

With respect to independent Claim 32, the Examiner has relied on Page 11 in Stevens and the rejection of Claim 1 to make a prior art showing of applicant's claimed technique "wherein a protocol-specific module processes each reassembled datagram based on an upper protocol layer employed by the reassembled datagram."

Applicant respectfully asserts that Page 11 in Stevens only discloses demultiplexing in which "an Ethernet frame is received at the destination host [and] starts its way up the protocol stack [where] all the headers are removed by the appropriate protocol box." Clearly, such disclosure of demultiplexing does not even suggest a "protocol-specific module [that] processes each **reassembled** datagram based on an upper protocol layer employed by the reassembled datagram" (emphasis added), as claimed.

In addition, as noted above with respect to the rejection of Claim 1, as relied on by the Examiner, Col. 13, lines 32-49 in Trcka merely discloses that a "Post-Capture

Processing Module 98 processes the packets based on protocol-specific packet fields." Clearly, only generally disclosing a module that processes packets based on protocol specific packet fields, as in Trcka, fails to meet applicant's claimed "protocol-**specific** module [that] processes each reassembled datagram based on an upper protocol layer employed by the reassembled datagram" (emphasis added), as claimed.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. Thus, a notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to dependent Claim 4 et al., the Examiner has relied on Col. 2, lines 16-24; Col. 3, lines 29-45; and Claim 7 in Cheriton to make a prior art showing of applicant's claimed technique "wherein the antivirus scanner terminates the transient packet stream if the reassembled segment is not infected with at least one of a computer virus and malware."

Specifically, the Examiner has argued that Cheriton teaches "generation and refinement of filters for stopping the attack packets, and forwarding these filters

upstream." Applicant respectfully disagrees and asserts that stopping attack packets does not meet, and even *teaches away* from applicant's claimed technique "wherein the antivirus scanner terminates the transient packet stream if the reassembled segment is **not** infected with at least one of a computer virus and malware" (emphasis added), as claimed.

In addition, applicant notes that the excerpts from Cheriton relied on by the Examiner merely disclose "filter[ing] harmful data" where "a netflow directory and flow analyzer are used to detect harmful network flows…which needs to be filtered" (Col. 3, lines 34-42), and "generating a filter to prevent packets corresponding to said detected potentially harmful network flows from passing through said second network device" (Claim 7). Thus, Cheriton clearly discloses filtering harmful data, and not a technique "wherein the antivirus scanner terminates the transient packet stream if the reassembled segment is **not** infected with at least one of a computer virus and malware" (emphasis added), as claimed.

With respect to dependent Claim 55, the Examiner has relied on Col. 14, lines 61-67 in Trcka to make a prior art showing of applicant's claimed technique "wherein the incoming datagrams include IP datagrams that are reassembled into TCP segments."

Applicant respectfully asserts that the excerpt from Trcka relied on by the Examiner only teaches that "[a]ny of a variety of known security checks can be performed on the packet data at this stage," such as performing "virus checking… on all incoming FTP (File Transfer Protocol) and HTTP files from unknown sites." Clearly, only disclosing performing security checks on packet data, as in Trcka, fails to even suggest "incoming datagrams include IP datagrams that are reassembled into TCP segments," as applicant claims.

Again, since at least the third element of the *prima facie* case of obviousness has not been met, as noted above, a notice of allowance or a proper prior art showing of all of

applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 56-57 below, which are added for full consideration:

"wherein the spoofed network packet spoofs an origin server by sending a legitimate packet in place of an infected packet" (see Claim 56); and

"wherein each of the protocol-specific scanning submodules is used for retrieving a re-assembled packet from an associated protocol-specific queue" (see Claim 57).

Again, a notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested. To this end, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P393).

Respectfully submitted,
Zilka-Kotab, PC

/KEVINZILKA/

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100